

392 HOMEWORK 6

1. Make a table showing how the polynomials $(x^n - 1)$ factorize into irreducibles over \mathbb{Q} for each $n = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$. Prove that the factors you find really ARE irreducible.

| n | Factors |
|-----|---|
| 1 | $(x - 1)$ |
| 2 | $(x - 1)(x + 1)$ |
| 3 | $(x - 1)(x^2 + x + 1)$ |
| 4 | $(x - 1)(x + 1)(x^2 + 1)$ |
| 5 | $(x - 1)(x^4 + x^3 + x^2 + x + 1)$ |
| 6 | $(x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$ |
| 7 | $(x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ |
| 8 | $(x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$ |
| 9 | $(x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$ |
| 10 | $(x - 1)(x^4 + x^3 + x^2 + x + 1)(x + 1)(x^4 - x^3 + x^2 - x + 1)$ |
| 11 | $(x - 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ |
| 12 | $(x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)(x^2 + 1)(x^4 - x^2 + 1)$ |

To prove that the factors really are irreducible, use question 2 for $x^{p-1} + x^{p-2} + \dots + x + 1$ for p prime. Note setting $y = -x$ this also proves that $x^2 - x + 1$ and $x^4 - x^3 + x^2 - x + 1$ are irreducible. This covers all the factors except $x^2 + 1, x^4 + 1, x^6 + x^3 + 1$ and $x^4 - x^2 + 1$. Setting $x = y + 1$ in the first two of these they transform to

$$y^2 + 2y + 2, y^4 + 4y^3 + 6y^2 + 4y + 2$$

hence they are irreducible by Eisenstein. This leaves $x^6 + x^3 + 1$ and $x^4 - x^2 + 1$. These ones are a little harder...

First let's do $x^4 - x^2 + 1$. It factors over the reals as

$$(x^2 + \sqrt{3}x + 1)(x^2 - \sqrt{3}x + 1).$$

Both these quadratics are irreducible over \mathbb{R} . So by uniqueness of factorization this is the only way it can factor over \mathbb{R} . Since they're not rational it must be irreducible over \mathbb{Q} .

Finally let's do $x^6 + x^3 + 1$. It has

$$e^{\pm 2\pi i/9}, e^{\pm 4\pi i/9}, e^{\pm 8\pi i/9}$$

as roots (think where it came from!). So over \mathbb{R} it factors into irreducibles as

$$(x^2 + 2 \cos(2\pi/9)x + 1)(x^2 + 2 \cos(4\pi/9)x + 1)(x^2 + 2 \cos(8\pi/9)x + 1).$$

Now by uniqueness of factorization, if it splits over \mathbb{Q} , the factors must these too - or else must be obtained from these by multiplying some pair of them together. Either way, one of these quadratics would have to belong to $\mathbb{Q}[x]$. Therefore we'll be done if we can show that $\cos(2\pi/9), \cos(4\pi/9)$ and $\cos(8\pi/9)$ are all irrational.

Let θ be one of $2\pi/9, 4\pi/9$ or $8\pi/9$. In all cases, $\cos(3\theta) = -1/2$. Let $y = 2 \cos \theta$. Then, if you remember the multiple angle formula, $\cos 3\theta = 4 \cos^3 \theta - \cos \theta$, we have that $y^3/2 - y/2 = -1/2$ in other words, $y^3 - y + 1 = 0$. We are trying to show that y is not rational. We will be done if we can show that the polynomial $x^3 - x + 1$ has no rational roots. But by the rational roots test, that is if and only if it has no integer roots, which you can convince yourself of by sketching the graph.

2. For which n is the polynomial $x^{n-1} + x^{n-2} + \dots + x + 1$ irreducible over \mathbb{Q} ? Make a conjecture and prove it.

It is irreducible if and only if n is prime. Proof. Suppose first that n is composite, say $n = pq$ for $p, q > 1$. Then,

$$x^{pq} - 1 = (x^p - 1)(x^{(p-1)q} + x^{(p-2)q} + \dots + x^q + 1).$$

So the irreducible factors of $x^{pq} - 1$ are all of degree $\leq (p-1)q < pq - 1$. Hence, since

$$x^{pq} - 1 = (x - 1)(x^{pq-1} + x^{pq-2} + \dots + x + 1)$$

the latter polynomial CANNOT be irreducible.

Conversely, suppose that p is prime. Then,

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \dots + x + 1).$$

Substitute $x = y + 1$ to get

$$(y + 1)^p - 1 = y((y + 1)^{p-1} + (y + 1)^{p-2} + \dots + (y + 1) + 1).$$

Expanding the left hand side using the binomial theorem then dividing through by y shows that

$$(y + 1)^{p-1} + \dots + (y + 1) + 1 = y^{p-1} + \binom{p}{1}y^{p-2} + \dots + \binom{p}{p-2}y + \binom{p}{p-1}.$$

Since p is prime, it must divide all the binomial coefficients here, and the constant term is p so not divisible by p^2 . Therefore it is irreducible by the Eisenstein criterion, so our original polynomial must be too.

3. For which n is the polynomial $x^n + 1$ irreducible over \mathbb{Q} ? Make a conjecture. Can you prove it? Try for a little while but don't worry if you cannot.

Conjecture. It is if and only if n is a power of 2.

4. There are two divisors of the number 2, namely, 1 and 2. There are three divisors of the number 4, namely, 1, 2 and 4. Compute the number of divisors of n for $n = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$. What has this got to do with the number of irreducible factors in your table? Make a conjecture – but don't try to prove it since it is rather hard.

For $n = 2, 3, 4, \dots, 12$ you get 2, 2, 3, 2, 4, 2, 3, 3, 4, 2, 6. This appears to be exactly the same as the number of irreducible factors in $(x^n - 1)$ according to the table.

5. Let $\phi(n)$ be the biggest degree of an irreducible factor of $x^n - 1$. For instance, $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$ so $\phi(4) = 2$. Using your table, compute $\phi(n)$ for $n = 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$.

For $n = 2, 3, 4, \dots, 12$ you get 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4.

6. There is just one unit in \mathbb{Z}_2 , there are two units in \mathbb{Z}_3 and in \mathbb{Z}_4 . Continue this sequence: how many units are there in \mathbb{Z}_n for $n = 4, 5, 6, 7, 8, 9, 10, 11, 12$. Make a conjecture comparing your answers to 5 and 6. We will prove your conjecture in class in a while, so you can assume it is a fact for the remainder of this homework sheet!

It looks like the number of units in \mathbb{Z}_n is equal to the biggest degree $\phi(n)$ of an irreducible factor of $x^n - 1$.

7. Prove that for p prime, the number of units in \mathbb{Z}_{p^n} is equal to $p^{n-1}(p - 1)$. (Hint: it is easier to count the number of non-units in \mathbb{Z}_{p^n} first.) Hence, assuming the conjecture you made in 6, you have shown that $\phi(p^n) = p^{n-1}(p - 1)$.

To count the number of non-units in \mathbb{Z}_{p^n} , we need to count the number of things from $1, 2, 3, \dots, p^n - 1, p^n$ that are not relatively prime to p^n , i.e. that are multiples of p . Here they are: $p, 2p, 3p, \dots, p^n - p, p^n$ or $1.p, 2.p, \dots, (p^{n-1} - 1).p, p^{n-1}.p$. There are p^{n-1} of them. Hence there are p^{n-1} non-units, so $p^n - p^{n-1} = p^{n-1}(p - 1)$ units.

8. What is $\phi(2^k)$? What is the irreducible factor of $x^{2^k} - 1$ of biggest degree? Now (assuming the conjecture you made in 6 is true) prove for any n that $x^n + 1$ is irreducible if and only if n is a power of 2.

By 7, $\phi(2^k) = 2^{k-1}$. So the irreducible factor of $x^{2^k} - 1$ of biggest degree must have degree 2^{k-1} . Since $x^{2^k} - 1 = (x^{2^{k-1}} - 1)(x^{2^{k-1}} + 1)$ and the first of the polynomials on the right hand side is reducible, it follows that $x^{2^{k-1}} + 1$ must be irreducible.

It remains to show that if n is not a power of 2 then $x^n + 1$ is reducible. Consider

$$x^{2n} - 1 = (x^n - 1)(x^n + 1).$$

The first of the polys on the RHS is reducible. So the second one is irreducible if and only if $\phi(2n) = n$. So we will be done if we can show that whenever n is not a power of 2, $\phi(2n) < n$.

Equivalently, by our conjecture, we need to show that LESS THAN half of the numbers on the list $1, 2, \dots, 2n$ are relatively prime to $2n$. Well, exactly half of them are divisible by 2, so not relatively prime. Moreover if n is not a power of 2, it has some odd prime factor p . But then p is not relatively prime to $2n$ either. So less than half are relatively prime, and we're done.